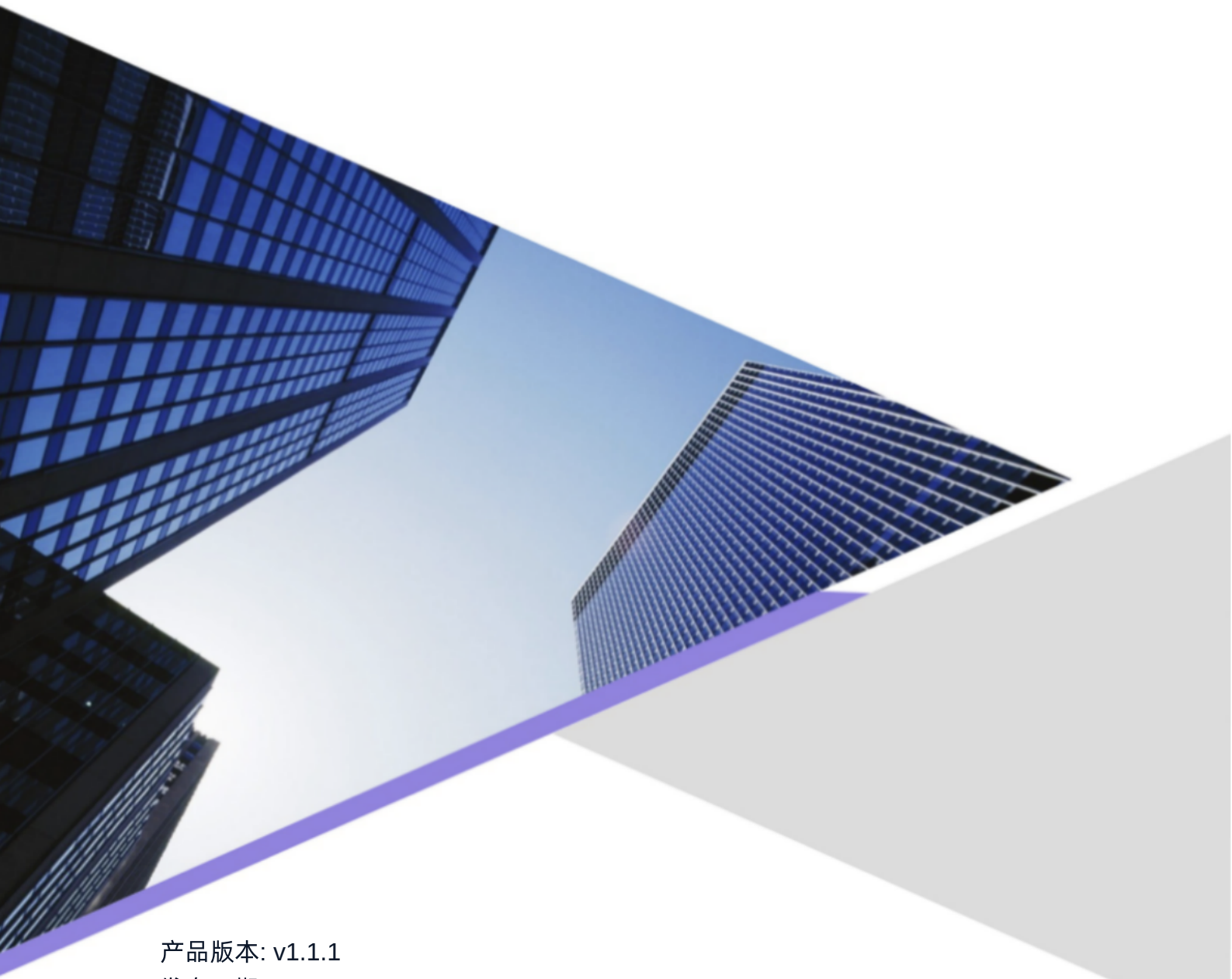
易捷行云
EasyStack

证书与密钥服务

产品介绍



产品版本: v1.1.1
发布日期: 2023-06-20

目录

1 产品介绍

1.1 什么是证书与密钥服务

证书与密钥服务是平台上提供私有CA、数字证书及密钥全生命周期管理的服务，帮助企业搭建和维护自己的CA体系，包括根及多级中间CA，同时，支持在企业内部签发和管理私有证书与密钥，托管企业购买的或第三方生成的证书。证书与密钥服务帮助企业无需花费高昂费用即可实现企业内部的应用身份认证和数据加解密，从而识别和保护组织内的应用程序、服务、设备和用户等资源。

产品优势

- **证书与密钥全生命周期管理**

  集成证书服务与密钥服务的一体化产品，可以通过简单的可视化操作建立完整的CA体系及密钥体系，并对其进行全生命周期的管理。

- **多种密钥算法支持**

  证书服务不仅支持RSA2048、RSA4096、ECC256、ECC384等多种国际密钥算法，符合PKI/CA国际标准，还支持SM2、SM3等国密算法。

  密钥服务不仅支持AES_256、RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384等国际算法，还支持SM2、SM4等国密算法。

- **双证书机制**

  支持签发双证书，即使用国密算法生成的签名证书和加密证书。签名证书在签名时使用，仅用来验证身份，加密证书在密钥协商时使用，其私钥和公钥由CA产生，并由CA保管。

- **证书托管**

  通过将本地的证书上传到证书服务，可以实现用户对证书的统一管理。

- **与云产品无缝集成**

  证书服务与独享型负载均衡云产品深度集成后，当负载均衡监听器使用HTTPS服务时，支持选择可用的证书提供统一交互体验。

密钥服务与身份与访问管理、计算、镜像、块存储等云产品集成后，可以统一管理用户的所有密钥，还可以进行本地数据的加解密和签名验签。

- **投入成本降低**

  私有证书服务能够避免高昂的商业证书开销，尤其在开发、测试阶段，通过使用免费证书就可以测试商业证书的功能，大幅降低IT成本。

  密钥服务提供统一的密钥管理策略和加密API给云产品服务使用，用户无需自建密码基础设施。

- **安全合规**

  密钥服务的密钥都由符合国家密码管理局认证的硬件加密机来执行密码学运算生成和存储，保证密钥的安全性和合规要求。

  私有CA服务能够签发客户端证书和服务端证书，提供端到端的加密，满足客户对安全场景的诉求。

主要功能

私有CA

- 支持私有证书颁发机构（私有CA），支持多种密钥算法，包括RSA2048、RSA4096、ECC256、ECC384、SM2，支持X.509 v3证书格式。
- 支持根CA和从属CA，根CA下可以包含多个从属CA，每个从属CA下可以包含多个下一级的从属CA，从而形成一套CA层次结构。
- 支持CA的全生命周期管理，包括启动、禁用、删除、下载等操作。

证书管理

- 支持创建、查看、编辑、下载、删除证书。支持多种密钥算法，包括RSA2048、RSA4096、ECC256、ECC384、SM2。
- 支持证书文件格式适配多种服务器类型，例如Tomcat、Nginx、Apache、IIS。
- 支持上传第三方生成的证书和私钥功能，实现在云平台统一管理各种证书、查看绑定证书域名和到期时间、修改证书名称、删除过期的证书等一站式服务，有效提高证书运维效率。

密钥管理

- 支持密钥产生、保存、分发和销毁等全生命周期的管理。
- 创建密钥支持多种密钥算法，包括AES_256、RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384等国际算法，以及SM2、SM4等国密算法，实现用户级隔离的数据加密保护。
- 支持信封加密，基于密钥管理系统的信封加密能力，可以对任意长度或大小的数据进行加密。
- 支持根据不同厂商的硬件加密机，动态返回密钥算法，包括对称密钥、非对称密钥以及Hash算法。
- 支持密钥计划删除功能，高危操作防护机制，防止密钥意外删除导致数据无法解密。

1.2 使用场景

- **保护企业信息化应用**

  建立统一的企业证书管理体系，实现证书全生命周期管理，融入持续监控和自动化管理能力，防范因证书管理不善导致的风险。并可以使用证书在企业内部进行应用身份认证和数据加解密。

- **数字身份认证**

  客户端证书是相对于服务器端而言，是用于证明客户端用户身份的数字证书，用户在与服务器端通信时可以证明其真实身份。适用于各种涉密系统、网上应用和网络资源的客户端强身份认证。

  客户端证书是一种更加安全的数字身份认证，通过客户端证书来代替用户名密码的形式安全地访问系统。

- **VPN Server使用客户端证书认证**

  VPN Server使用客户端证书认证机制替代传统的用户名和密码等形式，提升VPN安全，保护组织内部系统。

- **保护云平台服务数据的机密性和完整性**

  密钥服务的密钥使用经过国家密码管理局鉴定通过的硬件密码设备来生成和保护，使用密钥服务轻松创建和控制用于加密数据的密钥，与多个云产品服务集成，以帮助客户保护这些服务数据的机密性和完整性。

1.3 基本概念

本小节将介绍一些与数字证书相关的通用技术名词或原理。若已熟悉相关技术，可忽略本节内容；若尚不熟悉或对其中某部分不了解，可以阅读本小节进行了解。您也可以查阅更多专业资料以便深入了解。

加密与密钥

加密是保证数据传输安全性的一种手段，即使用密钥对明文数据进行加密处理，使其成为不可读的密文，密文通过密钥解密后可还原出明文。按照加解密使用的密钥是否相同，可划分密钥类型为对称加密和非对称加密两种。即相同的称为对称加密，不同的称为非对称加密。

数字证书的工作原理即为非对称加密。非对称加密使用到的两个不同的密钥通常被称为“公钥”和“私钥”。公钥加密的数据只能用私钥解密，同理，私钥加密的数据只能用公钥解密。私钥只能由使用者拥有与使用，不可泄漏，公钥可以公开给所有人。在本云平台创建私有证书时系统会自动生成证书文件和私钥文件，对应的公钥即保存在证书文件中。

数字签名与数字证书

在数据收发过程中，若要保证数据安全，需要考虑两个问题：如何证明发送内容没有被篡改、如何证明内容确实来自真正想要通信的对方。

第一个问题，为了保证传输的数据内容不被篡改，发送数据方需要基于数据计算出一个“指纹”，并将“指纹”与数据一同发送出去。这个“指纹”其实是使用哈希算法计算出内容的哈希值，这个哈希值是唯一的，且无法通过哈希值推导出内容。接受数据方收到消息后，也基于数据计算出一个“指纹”，并与发送者发来的指纹进行比对。如果一致则认为内容没有被篡改，如果不一致则证明内容可能被篡改过。

在这个过程中，虽然确保了内容没有被篡改过，但是无法保证“内容+哈希值”整体没有被人替换过，于是还需要考虑第二个问题，保证没有篡改过的数据确实来自真正想要通信的对方。

确认身份的第一种手段就是 数字签名，即发送方使用私钥对“指纹”进行加密。同时发送方需要公布自己的公钥。这样接收方如果能用该公钥解密，就说明消息是由持有私钥的人发的。但如果有恶意者伪造了公钥，恶意者拿着自己的公钥和私钥仍然可以冒充发送方与接收方通信，因此还需要引入一个第三方权威机构来证明公钥确实是来自发送方的。

发送方将自己的公钥与身份信息发送给CA（数字证书认证机构），CA使用自己的私钥对发送方的公钥和身份信息等内容进行数字签名，并把“身份等信息+公钥+数字签名”打包成一个 数字证书。通信过程中发送方向接收方展示自己的数字证书，接收方使用CA的公钥（通常浏览器和操作系统中集成了权威CA的公钥）解密证书

中的数字签名得到哈希值，再与计算出的哈希值对比，若一致则证明公钥确实来自真正的发送方而非恶意者冒充。此时接收方可以使用保存在证书中的发送方的公钥进行后续的通信。

至此，即可保证收到的数据确实来自正确的发送方且未被篡改过。

通常，向互联网上认可的权威CA机构申请证书是需要高昂费用的，因此有时需要使用私有证书，私有证书虽然在互联网上不受信任，但是可满足企业内部应用数据需要密码技术提供加密的需求。

数字证书与HTTPS

HTTPS是一种基于SSL协议的网站加密传输协议，网站安装数字证书后，可以使用HTTPS加密协议访问，实现了客户端与服务端之间的加密通信通道，防止传输数据被泄露或篡改。简单来说，HTTPS是HTTP的安全加强版，而想要使用HTTPS，则需先安装数字证书。

1.4 产品获取

前提条件

在执行下述产品获取操作步骤前，请确保以下条件均已满足：

- 如需获取正式版云产品，请提前将已获取的许可文件准备就绪。

操作步骤

1. 获取并安装“证书与密钥服务”云产品。

   在顶部导航栏中，依次选择[产品与服务]-[产品与服务管理]-[云产品]，进入“云产品”页面获取并安装“证书与密钥服务”云产品。具体操作说明，请参考“产品与服务管理”帮助中“云产品”的相关内容。

2. 访问证书与密钥服务。

   在顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]，选择各子菜单，即可访问对应服务。

1.5 权限说明

本章节主要用于说明证书与密钥服务各功能的用户权限范围。其中，√ 代表该类用户可对云平台内所有项目的操作对象执行此功能，**XX项目** 代表该类用户仅支持对XX项目内的操作对象执行此功能，未标注代表该类用户无权限执行此功能。

功能		云管理员	部门管理员/项目管理员/普通用户
私有CA	信息展示	√	仅已加入项目
	创建私有CA	仅Default/admin项目	
	导出	√	
	启用/禁用	√	
	编辑	√	
	下载	√	
	删除	√	
证书管理	信息展示	√	仅已加入项目
	创建私有证书	仅Default/admin项目	
	导出	√	
	上传证书	仅Default/admin项目	
	下载	√	
	编辑	√	
	删除	√	
密钥管理	信息展示	仅该用户创建对象	仅该用户创建对象

	功能	云管理员	部门管理员/项目管理员/普通用户
	创建密钥		
	编辑		
	对称密钥在线加密/解密		
	导出		
	启用/禁用		
	删除		
	取消计划删除		

1.6 使用限制

- 对于私有CA，其层级结构最多支持8级。
- 对于对称密钥在线加密/解密功能，输入的数据长度不能超过512个字符。

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区1号楼1层107-2号
南京易捷思达软件科技有限公司：
江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)